REMARKS

In the Office Action, the Examiner rejected Claims 1-13, which were all of the then pending claims, under 35 U.S.C. §103 as being unpatentable over the prior art, principally U.S. Patents 5,592,553 (Guski, et al.) and 6,141,760 (Abadi, et al.). More specifically, Claims 1, 6 and 8-10 were rejected as being unpatentable over Guski, et al. in view of Abadi, et al; and Claims 2, 7 and 11 were rejected as being unpatentable over Guski, et al. and Abadi, et al. and further in view of portions of a textbook "Applied Cryptography" (Schneier). Claims 3-5, 12 and 13 were rejected over Guski, et al. in view of Abadi, et al. and further in view of a reference identified as "Cheng."

Applicant notes that "Cheng is not further identified in the Office Action, and applicant requests that the Examiner more specifically identify this reference.

Applicant is herein amending Claims 1 and 10 to better define the subject matters of these claims. Also, Claim 2 is being amended to improve the form of the claim, and Claim 14, which is dependent from Claim 2, is being added to describe a preferred feature of the invention.

For the reasons discussed below, Claims 1-14 patentably distinguish over the prior art and are allowable. The Examine is, accordingly, respectfully requested to reconsider and to withdraw the rejections of Claims 1-13, and to allow these claims and new Claim 14.

The present invention, generally, relates to a method and device for reading in a password to a computer system in a secure manner. As discussed in detail in the present application, the use of passwords to gain access to computer and computer systems has

become very common. However, despite this widespread, general acceptance, there still are a number of problems with the use of computer passwords.

This invention effectively addresses a number of these problems. For instance, one important problem that is effectively addressed by this invention is the use of rouge software, such as a Trojan Horse, to hijack or steal a password when it is entered into the computer. The invention addresses this by putting a software generator module in the operating system of the computer, in series between a user who is inputting the password and the program being accessed. This generator module encrypts the password, and then the encrypted password is sent to the program, allowing access to that program.

The primary prior art references, Guski, et al. and Abadi, et al, relied on by the Examiner to reject the claims provide various procedures and system for improving the security of passwords. However, neither of these references addresses the same problem that is addressed by this invention in the same wary as the present invention does.

For example, Guski, et al. describes a procedure in which passwords are used one-time only. The passwords change pseudorandomly, for example as a function of time, with each request for authentication. More specifically, at a requesting node, a non-time dependent value is generated from nonsecret information identifying the user and a host application, using a secret encryption key shared with an authenticating node. This non-time dependent value is combined with a time-dependent value to generate a composite value that is encrypted to produce an authentication parameter. This authenticating password is reversibly transformed into an alphanumeric character string that is transmitted as a one-time password to the authenticating node.

The advantage of using such a tone-time password is that, even if the password is intercepted, it cannot be later used to gain access to the computer system.

Abadi, et al. discloses a method for generating unique passwords. In this procedure, several values, for example, a master password, an access password and a user name, are combined to produce a unique password. In this way, common passwords or passwords that might be used by more than one person, are converted to unique passwords.

Neither of these references addresses the above-discussed problem – preventing a password from being improperly obtained – that is addressed by the present invention. Also, neither of these references discloses or suggests the unique use of the generator module of the present invention – that is, the use of the generator module, as part of the computer's operating system, in series between a user and a program being accessed, to encrypt the user password and to pass that encrypted password to the program. It is this use of the generator module in this way that, among other advantages, substantially improves the security of the password.

Independent Claims 1 and 10 describe the above-discussed feature of the invention. In particular, both of these claims describe a computer including an operating system having a generator module, and both of these claims indicate that the generator module receives a program specific identifier from a program, receives the password, and generates a program-password-specific identifier from the program specific identifier and the password.

As explained above, neither Guski, et al., nor Abadi, et al discloses or suggests this feature of the invention.

The other references of record have been reviewed, and they too, whether considered individually or in combination, also do not disclose or suggest this use of a generator module.

Because of the above-discussed differences between Claims 1 and 10 and the prior art, and because of the advantages associated with these differences, Claims 1 and 10 patentably distinguish over the prior art and are allowable. Claims 2-7 and 14 are dependent from Claim 1 and are allowable therewith; and Claims 11-13 are dependent from, and are allowable with, Claim 10. Also, Claims 8 and 9 incorporate by reference the method steps described in Claim 1, and thus Claims 8 and 9 patentably distinguish over the prior art for the same reasons advanced above in connection with Claim 1.

Accordingly, the Examiner is respectfully asked to reconsider and to withdraw the rejections of Claims 1-13 under 35 U.S.C. §103, and to allow these claims and new Claim 14.

If the Examiner believes that a telephone conference with Applicant's Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,

John S Sensny

John S. Sensny
Registration No. 28,757
Attorney for Applicant

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza – Suite 300
Garden City, New York 11530
(516) 742-4343

JSS:jy